DERWENT-ACC-NO: 1997-282091
DERWENT-WEEK: 199726

TITLE: Access authorisation misuse recognition method - overwrites variable
data at least partly by new data generated from evaluating unit, transmitted to
memory and required in next interaction of evaluating unit as new key word

INVENTOR: SCHEINERT, S

PATENT-ASSIGNEE: SCHEINERT S[SCHEI]

PRIORITY-DATA: 1995DE-1042732 (November 16, 1995)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
DE 19542732 A1	May 22, 1997	N/A	004	G07C 011/00

APPLICATION-DATA:

PUB-NO	APPL-DESCRIPTOR	APPL-NO	APPL-DATE
DE19542732A1	N/A	1995DE-1042732	November 16, 1995

INT-CL_(IPC): G07C009/00; G07C011/00 ; H04Q007/34

ABSTRACTED-PUB-NO: DE19542732A
BASIC-ABSTRACT: The method concerns the use of chip cards for access to some
service or installation and the use of writing and reading units for evaluating
and checking the identity of the person possessing the card, in association
with a central computer of the service or the monitoring equipment.

These units read the data in the card and pass the data to the

evaluating and
deciding unit. Depending on the result, access to the facility or service is
granted or refused. Each interaction generates a dynamic key for the next
interaction or transaction, and this cannot be known by any unauthorised
person, but only by the subscriber's station from the last transaction.

USE/ADVANTAGE - Suitable for identity, credit and payment cards. Improvement
in security.

CHOSEN-DRAWING: Dwg.0/0

TITLE-TERMS:
ACCESS AUTHORISE MISUSE RECOGNISE METHOD VARIABLE DATA NEW DATA GENERATE
EVALUATE UNIT TRANSMIT MEMORY REQUIRE INTERACT EVALUATE UNIT NEW KEY WORD

DERWENT-CLASS: T05 W01

EPI-CODES: T05-D01A; T05-E; T05-H02C; W01-A05B;

SECONDARY-ACC-NO:
Non-CPI Secondary Accession Numbers: N1997-233516

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 195 42 732 A 1**

(51) Int. Cl.[6]:
G 07 C 11/00
G 07 C 9/00
H 04 Q 7/34

(21) Aktenzeichen: 195 42 732.7
(22) Anmeldetag: 16. 11. 95
(43) Offenlegungstag: 22. 5. 97

(71) Anmelder:
Scheinert, Stefan, 90443 Nürnberg, DE

(74) Vertreter:
Matschkur Götz Lindner, 90402 Nürnberg

(72) Erfinder:
gleich Anmelder

(56) Entgegenhaltungen:
US 49 74 193
EP 05 39 763 A2
JP 7-81521 (A), mit zugehörigem Eintrag aus Datenbank WPIDS;

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zur Erkennung des Mißbrauchs einer Zugangsberechtigung

(57) Die Erfindung richtet sich auf ein Verfahren zum Erkennen der unerlaubten Benutzung einer zum Zugriff auf eine Dienstleistungsanlage, zum Zugang zu Räumen o. dgl. berechtigenden Identifizierung mit einem personenbezogenen Speichermedium und mit einer Schreib-/Leseeinrichtung für dieses Speichermedium, wobei die Schreib-/Leseeinrichtung mit einer Auswerte- und Entscheidungseinrichtung kommuniziert, wobei zur Überprüfung der Identifizierung in dem personenbezogenen Speichermedium gespeicherte Daten gelesen und an die Auswerte- und Entscheidungseinrichtung übertragen werden, welche in Abhängigkeit von diesen Daten eine Interaktion gewährt oder verweigert, und wobei mindestens ein Teil der übertragenen Daten variabel ist; erfindungsgemäß werden die variablen Daten bei jeder Interaktion zumindest teilweise durch neue Daten überschrieben, die von der Auswerteeinrichtung generiert und zu dem Speichermedium übertragen werden, und die bei der nächsten Interaktion von der Auswerte-/Entscheidungseinrichtung als neues Schlüsselwort zur Identifizierung verlangt werden.

DE 195 42 732 A 1

195 42 732 A 1

Beschreibung

Die Erfindung richtet sich auf ein Verfahren zum Erkennen der unerlaubten Benutzung einer zum Zugriff auf eine Dienstleistungsanlage, zum Zugang zu Räumen od. dgl. berechtigenden Identifizierung mit einem personenbezogenen Speichermedium, einer Schreib-/Leseeinrichtung für dieses Speichermedium und einer Auswerte- und Entscheidungseinrichtung, wobei zur Identifizierung in dem personenbezogenen Speichermedium gespeicherte, variable Daten gelesen und an die Auswerte- und Entscheidungseinrichtung übertragen werden.

Insbesondere bei Mobilfunknetzen ist die Gefahr eines Mißbrauchs relativ groß, denn hier kann eine Manipulation an einem Endgerät nicht erkannt werden, außerdem lassen sich manipulierte Endgeräte aufgrund ihrer Mobilität viel intensiver nutzen als bspw. stationäre Telefonanschlüsse, so daß der entstehende Schaden bei Mobilfunknetzen weitaus größer sein kann.

Zur Vermeidung eines Mißbrauchs von Mobilfunknetzen sind daher eine Reihe von Sicherheitsvorkehrungen vorgesehen: Jeder Teilnehmer besitzt eine sog. Chip-Karte, mit für ihn charakteristischen Daten, die er zunächst in ein Endgerät (Handy) einsetzen muß, um dieses in Betrieb nehmen zu können. Sofern der Teilnehmer mit dem Mobilfunknetz in Interaktion treten will, d. h., zur Durchführung eines Gesprächs auf dieses zugreifen will, muß er zunächst seine persönliche Identifikationsnummer eingeben, welche das Handy nun mit den auf der eingesetzten Chip-Karte gespeicherten Daten vergleicht. Stimmt diese Zahl überein, so erkennt das Handy die Identität des Teilnehmers und tritt nun in Kommunikation mit einer Zentrale des Mobilfunknetzes, um einen Gesprächskanal zu erhalten. Zu diesem Zweck funkt das Handy eine Identifikationsnummer; daraufhin antwortet die Zentrale durch Übertragung einer Zufallszahl X. Nun unterwirft das Handy die empfangene Zufallszahl X einer auf der Chip-Karte abgespeicherten Schlüsselfunktion Y und generiert solchermaßen eine Ergebniszahl Z. Diese wird zur Zentrale gefunkt, welche das Ergebnis Z mit einem intern errechneten Referenzwert vergleicht und bei Identität dieser beiden Werte den Zugriff auf das Mobilfunknetz freigibt und einen Gesprächskanal zuteilt. Dieses Verfahren soll einem Mißbrauch des Mobilfunknetzes vorbeugen, indem selbst durch Abhören von Kontrollkanälen und der darauf folgenden Erkennung von Teilnehmernummern dennoch die Schlüsselfunktion Y unbekannt bleibt, so daß ein Betrüger niemals die richtige Antwort Z auf die jeweils unterschiedliche Zufallszahl X senden kann. Es ist jedoch möglich, in betrügerischer Absicht eine 1 : 1-Kopie einer Chip-Karte anzufertigen und dabei auch die interne Schlüsselfunktion Y zu kopieren, die eine Bestimmung des jeweils richtigen Ergebnisses Z und somit einen Mißbrauch der betreffenden Teilnehmer-Identifizierung zuläßt.

Um auch hier einen verbesserten Schutz vor Mißbrauch zu bieten, sieht die DE-PS 34 48 393 vor, daß sowohl in der Teilnehmerstation wie auch in der Zentrale des Mobilfunknetzes zusätzliche, veränderbare Daten vorhanden sind, wobei zum Verbindungsaufbau die betreffenden Daten von der Teilnehmerstation zur Zentrale übertragen werden, um dort miteinander verglichen zu werden. Hierbei ist vorgesehen, daß als veränderbare Daten die Zahl von erfolgreichen Verbindungsaufbauten der Teilnehmerstation verwendet wird, und daß in der Teilnehmerstation wie auch in der Zentrale

jeweils ein Zähler angeordnet ist, welche Zähler bei jedem erfolgreichen Verbindungsaufbau inkrementiert werden. Hier wird anstelle des fest vorgegebenen Schlüssels ein variabler Zählerstand verwendet, der sich mit jedem Telefongespräch verändert. Man erhält dadurch sozusagen einen "dynamischen" Schlüssel, der folgenden Vorteil hat: Wird eine 1 : 1-Kopie der betreffenden Chip-Karte angefertigt, ist zunächst der Zählerstand auf der kopierten Karte richtig; bei der nun folgenden Benutzung der betrügerisch angefertigten Karte wird zunächst auch das Schlüsselwort immer richtig inkrementiert, so daß mehrere Gespräche möglich sind. Sobald jedoch die Original-Chip-Karte wieder benutzt wird, kann die Zentrale an dem übertragenen, falschen Zählerstand erkennen, daß ein Zweitgerät dieselbe Identifizierung benutzt. Daraufhin fragt die Zentrale eine zweite Kennung ab, um das Originalgerät herauszufinden, und sobald dies geschehen ist, kopiert die Zentrale dessen Teilnehmernummer, so daß nun der bereits hochgezählte Zählerstand der betrügerischen Kopie falsch ist. Bei diesem Verfahren mit "dynamischem" Schlüssel kann zwar ein Mißbrauch erkannt und vorübergehend ausgeschlossen werden. Sobald der Betrüger jedoch eine Diskrepanz seines Zählerstandes erkennt, kann er durch manuelles Herabzählen seines Zählers versuchen, den aktuellen Zählerstand der Zentrale herauszufinden, und sich dann abermals in das Mobilfunknetz einschmuggeln.

Aus diesen Nachteilen des vorbekannten Stands der Technik resultiert das die Erfindung initiierende Problem, ein Verfahren zum Erkennen des Mißbrauchs einer Zugangs- oder Zugriffsberechtigung in Form einer auf einem personenbezogenen Speichermedium gespeicherten Identifizierung dahingehend zu verbessern, daß selbst bei einer 1 : 1-Kopie des Speichermediums und/oder bei Verwendung eines "intelligenten" Nachbaus eines derartigen Speichermediums keinerlei Möglichkeit eines dauerhaften Mißbrauchs besteht.

In Verfolgung dieses Ziels sieht die Erfindung vor, daß die zur Identifizierung vor jeder Interaktion übertragenen, variablen Daten bei jeder Interaktion zumindest teilweise durch neue Daten überschrieben werden, die von der Auswerteeinrichtung generiert und zu dem Speichermedium übertragen werden, und die bei der nächsten Interaktion von der Auswerte-/Entscheidungseinrichtung als neues Schlüsselwort zur Identifizierung verlangt werden. Die Erfindung geht hierbei aus von der Idee eines "dynamischen" Schlüssels, überläßt es jedoch nicht der betreffenden Teilnehmerstation, das nächste Schlüsselwort selbst zu generieren, sondern erzeugt das nächst folgende Schlüsselwort auf völlig unvorhersehbare Art selbst und überträgt es sodann auf die Teilnehmerstation, welche dieses bis zur nächsten Interaktion speichert. Hierdurch kann das nächstfolgende Schlüsselwort von keiner anderen Teilnehmerstation als eben dieser ermittelt werden, weder durch eine 1 : 1-Kopie der betreffenden Chip-Karte, noch durch einen "intelligenten" Nachbau mit bspw. eingebauter Dekrementierfunktion eines Zählers od. dgl. Eine in betrügerischer Absicht angefertigte 1 : 1-Kopie einer Chip-Karte wird spätestens dann erkannt, wenn die zur Benutzung berechtigte Person ihre Originalkarte mit dem alten Schlüsselwort benutzt. Sobald diese daraufhin ein neues Schlüsselwort erhalten hat, ist es für die 1 : 1-Kopie niemals mehr möglich, den richtigen Schlüssel herauszufinden. Dies ist dadurch sichergestellt, daß die von der Auswerteeinrichtung generierten Daten auf völlig unvorhersehbare Art, bspw. mit einem Zufallsgenerator

erzeugt werden.

Um zu erkennen, wieviele der zuletzt geführten Gespräche auf das Konto der betrügerisch angefertigten 1 : 1-Kopie zu rechnen sind, ist erfindungsgemäß weiterhin vorgesehen, daß ein anderer Teil der variablen Daten bei jeder Interaktion durch einen Zählerbaustein inkrementiert wird, wobei dieser Teil der variablen Daten zur Übertragung ggf. verschlüsselt werden kann. Hierdurch ist es der Zentrale eines Mobilfunknetzes bspw. möglich, die Differenz der Zählerstände ihres Zählers minus des Zählers der als Original erkannten Teilnehmerstation zu bilden, wobei diese Differenz die Anzahl der betrügerisch geführten Gespräche angibt. Nun können die betreffenden Gebühreneinheiten von der Rechnung des Originalteilnehmers subtrahiert werden, so daß dieser von dem Betrugsversuch keinen Schaden hat.

Um die tatsächlich zugangsberechtigte Person von dem Betrüger zu unterscheiden, können in der Auswerteeinrichtung ein Paßwort und/oder personenbezogene Daten gespeichert sein, welche ausschließlich der zugangsberechtigten Person bekannt sind und deren manuelle oder verbale Eingabe die Vergabe eines neuen Schlüsselworts an diese Original-Chip-Karte veranlaßt, unabhängig davon, ob das von dieser zuletzt gelesene Schlüsselwort richtig war oder nicht. Die Abfrage eines Paßworts oder personenbezogener Daten kann dabei bevorzugt von einem Bediensteten des Systembetreibers vorgenommen werden, dem neben dieser Tätigkeit eine Reihe weiterer Aufgaben übertragen sein können. Zur Erhöhung der Sicherheit gegenüber Betrügern kann während eines derartigen Gesprächs, insbesondere während der Nennung eines Paßworts, eine Stimmenanalyse durchgeführt werden, mit deren Hilfe sich zuverlässig überprüfen läßt, ob die betreffenden Daten tatsächlich von der berechtigten Person stammen.

Um eine betrügerische Chip-Karte ein für allemal zu entwerten, wird aufgrund einer falschen Identifizierung jegliche weitere Interaktion verweigert, so daß keinerlei Kosten anfallen. Es ist jedoch auch möglich, dieser betrügerischen Station eine richtige Identifizierung vorzutäuschen und das bspw. folgende Telefongespräch aufzuzeichnen, um daraus Rückschlüsse über den Betrüger zu gewinnen.

Um auch bei der Initialisierungsphase einer erfindungsgemäßen Chip-Karte die Vergabe eines Paßworts an eine betrügerisch erstellte Chip-Karte auszuschließen, kann gemäß einer bevorzugten Weiterbildung der Erfindung das Paßwort bei einer erstmaligen Interaktion von dem Speichermedium gelesen und in der Auswerteeinheit gespeichert und sodann auf dem Speichermedium vollständig gelöscht werden. Hierdurch erfolgt ausschließlich ein Datentransfer von der Mobilstation zur Zentrale, niemals dagegen in umgekehrter Richtung. Indem das Paßwort sodann auf dem Speichermedium gelöscht wird, kann es selbst bei einer 1 : 1-Kopie nicht mehr aufgefunden werden.

Die Erfindung ist nicht auf Mobilfunknetze beschränkt, sondern kann auch bei anderen Dienstleistungsanlagen wie Telefonnetzen, bankeigenen Netzen von Geldausgabeautomaten, (firmeneigenen) Computernetzen oder -systemen od. dgl. vorteilhaft eingesetzt werden. Voraussetzung ist ausschließlich die Vergabe von personenbezogenen Speichermedien an zum Zugang oder zum Zugriff berechtigte Personen, um diese identifizieren zu können. Während bei öffentlichen Telefonen, Geldausgabeautomaten od. dgl. eine Kommunikation zwischen dem Speichermedium und der betreffenden Zentrale der Dienstleistungsanlage ausschließlich zum Zweck eines Zugriffs auf diese Dienstleistungsanlage erfolgt, so daß als Interaktion tatsächlich nur ein erfolgreicher Zugriff anzusehen ist, laufen in Mobilfunknetzen regelmäßig systeminterne Funktionen ab, die ebenfalls als Interaktionen im Sinne der Erfindung angesehen werden können, welche eine Aktualisierung der variablen Daten ermöglichen. Bei diesen systeminternen Funktionen handelt es sich bspw. um die in regelmäßigen Zeitabständen erfolgende Rückmeldung einer Teilnehmerstation, um in einer Kontrolliste in der Zentrale des Mobilfunknetzes ihre Kommunikationsbereitschaft zu signalisieren. Eine weitere Kommunikation zwischen Mobilstation und Funknetz findet immer dann statt, wenn die Mobilstation eine Funkzone verläßt und sich infolge der nachlassenden Empfangsfeldstärke eine andere Feststation auswählt. Auch bei dieser als Roaming bezeichneten Zuordnung ist eine Identifizierung der Teilnehmerstation notwendig, bei der anschließend die variablen Daten überschrieben werden können. Die Aktualisierung der variablen Daten bei jeder derartigen, systeminternen Funktion stellt sicher, daß ein betrügerisches Zweitgerät innerhalb eines kürzesten Zeitintervalls erkannt wird, selbst wenn die zugangsberechtigte Person über einen größeren Zeitraum hinweg nicht selbst auf das Mobilfunknetz zugreift. Hierdurch läßt sich der wirtschaftliche Schaden betrügerischer Aktivitäten auch für den Betreiber des Mobilfunknetzes auf einen vernachlässigbar niedrigen Betrag reduzieren.

Patentansprüche

1. Verfahren zum Erkennen der unerlaubten Benutzung einer zum Zugriff auf eine Dienstleistungsanlage, zum Zugang zu Räumen od. dgl. berechtigenden Identifizierung mit einem personenbezogenen Speichermedium, insbesondere in Form einer Chip-Karte, und mit einer Schreib-/Leseeinrichtung für dieses Speichermedium, wobei die Schreib-/Leseeinrichtung mit einer Auswerte- und Entscheidungseinrichtung, bspw. in Form einer Steuerzentrale oder eines Zentralcomputers der Dienstleistungs- oder Raumüberwachungsanlage kommuniziert, wobei zur Überprüfung der Identifizierung in dem personenbezogenen Speichermedium gespeicherte Daten gelesen und an die Auswerte- und Entscheidungseinrichtung übertragen werden, welche in Abhängigkeit von diesen Daten eine Interaktion, insbesondere den Zugriff/Zugang oder eine systeminterne Funktion, gewährt oder verweigert, und wobei mindestens ein Teil der übertragenen Daten variabel ist, **dadurch gekennzeichnet**, daß die variablen Daten bei jeder Interaktion zumindest teilweise durch neue Daten überschrieben werden, die von der Auswerteeinrichtung generiert und zu dem Speichermedium übertragen werden, und die bei der nächsten Interaktion von der Auswerte-/Entscheidungseinrichtung als neues Schlüsselwort zur Identifizierung verlangt werden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die von der Auswerteeinrichtung generierten Daten auf völlig unvorhersehbare Art, bspw. mit einem Zufallsgenerator, erzeugt werden.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß ein anderer Teil der variablen Daten bei jeder Interaktion durch einen Zählerbaustein inkrementiert wird, wobei dieser Teil der variablen Daten zur Übertragung ggf. verschlüsselt

werden kann.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß in der Auswerteeinrichtung ein Paßwort und/oder personenbezogene Daten gespeichert ist (sind), welche(s) ausschließlich der zugriffs-/zugangsberechtigten Person bekannt ist (sind), und dessen (deren) manuelle und/oder verbale Eingabe die Vergabe eines neuen Schlüsselworts an das dieser Person zugeordnete Speichermedium veranlaßt, unabhängig davon, ob das zuletzt gelesene Schlüsselwort richtig war oder nicht.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß bei Abweichung der variablen Daten von den der Auswerte-/Entscheidungseinheit bekannten Soll-Daten der Zugriff/Zugang mit der betreffenden Identifizierung verweigert wird, bis sich die zugangsberechtigte Person mittels des nur ihr bekannten Paßworts und/oder durch Eingabe weiterer, personenbezogener Daten ausgewiesen und daraufhin einen neuen Satz variabler Daten erhalten hat.

6. Verfahren nach Anspruch 4 oder 5, dadurch gekennzeichnet, daß das Paßwort bei einer erstmaligen Interaktion von dem Speichermedium gelesen und in der Auswerteeinheit gespeichert und sodann auf dem Speichermedium vollständig gelöscht wird.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Dienstleistungsanlage ein Mobilfunk- oder Telefonnetz, das bankeneigene Netz von Geldausgabeautomaten, ein (firmeneigenes) Computernetz oder -system od. dgl. ist.

8. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Dienstleistungsanlage ein Mobilfunknetz ist, dadurch gekennzeichnet, daß die variablen Daten vor Beginn eines Verbindungsaufbaus und/oder in regelmäßigen Zeitabständen (Timer-Ablauf) und/oder beim Zuordnen zu einer neuen Funkzone (Rooming) durch neue Daten überschrieben werden.